A Study on Cryptographic Protocols: Achieving Strong Security for Zero-knowledge Proofs and Secure Computation(Abstract_要旨)

AUTHOR(S):

Kiyoshima, Susumu

（ 続紙 １ ）

京都大学	博士（情報学）	氏名	清島　奨
論文題目	A Study on Cryptographic Protocols: Achieving Strong Security for Zero-knowledge Proofs and Secure Computation (暗号プロトコルに関する研究：ゼロ知識証明と秘密計算における高度な安全性の実現について)		

（論文内容の要旨）

本論文は代表的な暗号プロトコルであるゼロ知識証明と秘密計算に関するものであり，特に同時実行安全性や耐漏洩安全性等の高度な安全性を満たすゼロ知識証明および秘密計算について論じるものである。ここで，ゼロ知識証明は命題が真であること以外の情報を漏らすことなく証明を行う暗号プロトコルであり，秘密計算は複数のプロトコル参加者が持つ秘密入力に関し任意の関数の計算を行う暗号プロトコルである。同時実行安全性は暗号プロトコルの複数インスタンスが同時に実行される時の安全性であり，耐漏洩安全性はサイドチャネル攻撃と呼ばれる攻撃に対しプロトコル参加者の内部状態（秘密入力およびプロトコルで使用した乱数）の部分情報が攻撃者に漏洩することを防ぐ安全性である。

第１章では研究の背景および結果の概要が述べられている。特に，研究の背景ではまずゼロ知識証明および秘密計算の概念が説明され，次に（１）厳密な安全性定義・計算量仮定の下での数学的安全性証明が暗号技術の安全性の信頼度を高めるために重要であること，（２）暗号技術の応用先を広げるために同時実行安全性を始めとした高度な安全性の実現が重要となること，そして（３）高度な安全性を効率や計算量仮定の面で低コストに実現することが暗号理論における主要な研究方針の一つであることが述べられている。また，結果の概要ではまず本論文の主題が同時実行安全性または耐漏洩安全性を満たすゼロ知識証明および秘密計算を効率や計算量仮定の面で低コストに実現すること（そしてそれにより同時実行安全性および耐漏洩安全性の実現コストに関し一般的結果を得ること）であることが述べられ，次に本論文で示される四つの結果の各々について背景を含めて結果の概要が述べられている。

第２章では第３章以降で使われる記法や定義，既存暗号技術方式が与えられている。

第３章では最も強力な同時実行安全性をもつゼロ知識証明であるstatistical concurrent non-malleableゼロ知識証明に関する結果が与えられており，特に通常のゼロ知識証明に対して必要とされている仮定のみを用いてstatistical concurrent non-malleableゼロ知識証明を実現できることが示されている。つまり，本章ではstatistical concurrent non-malleableゼロ知識証明が通常のゼロ知識証明と比べ仮定に関する追加のコスト無しに実現可能であることが示されている。

第４章では耐漏洩安全性を満たすゼロ知識証明である耐漏洩ゼロ知識証明に関する結果が与えられている。特に，効率の代表的指標であるラウンド効率が漸近的に最適である方式（つまり，ラウンド効率がセキュリティパラメータと呼ばれるパラメータに依存しない定数である方式）が従来よりも弱い仮定（具体的には衝突困難ハッシュ関数の存在）のみを用いて構成可能であることが示されている。

第５章では非ブラックボックスゼロ知識証明と呼ばれるゼロ知識証明に関する結果が与えられており，特に同時実行安全性を満たす非ブラックボックスゼロ知識証明の

新しい方式が与えられている。非ブラックボックスゼロ知識証明は非ブラックボックスシミュレーションと呼ばれる手法で安全性が証明されているゼロ知識証明であり，同時実行安全性を持つ非ブラックボックスゼロ知識証明は同時実行安全性に関する様々な未解決問題の解決（例えば定数ラウンド同時実行安全ゼロ知識証明の実現）に必要であることが知られている。本章で与えられている方式は既存方式と比べ簡潔な安全性証明が可能という特徴を持つ。

第６章では同時実行安全性を満たす秘密計算に関しブラックボックス構成と呼ばれる性質を満たす方式が与えられている。ブラックボックス構成は方式の構成方法に関する性質であり，ブラックボックス構成である方式は計算量が小さくなることが多いという特徴を持つ。本章で提案されている方式はブラックボックス構成である既存方式と比べるとラウンド効率が良く，さらにブラックボックス構成ではない既存方式と比べても同等のラウンド効率を持っている。

第７章では本論文の結果のまとめと今後の課題が与えられている。

注）論文内容の要旨と論文審査の結果の要旨は１頁を３８字×３６行で作成し、合わせて、３，０００字を標準とすること。
論文内容の要旨を英語で記入する場合は、４００～１，１００wordsで作成し
審査結果の要旨は日本語５００～２，０００字程度で作成すること。

（続紙 ２ ）

（論文審査の結果の要旨）

ゼロ知識証明と秘密計算はどちらも暗号理論における中心的な暗号プロトコルであり，また同時実行安全性と耐漏洩安全性はどちらも理論的・実用的な重要性をもつ安全性である。

本論文は同時実行安全性や耐漏洩安全性を満たすゼロ知識証明および秘密計算に関する研究をまとめたものであり，特に方式の効率や安全性証明の仮定の面でコストを最小化するという問題に関連する四つの成果で構成されている。本論文が示す四つの成果はいずれも暗号プロトコル分野において重要度の高い問題に対するものである。また，ゼロ知識証明が秘密計算の重要な構成要素であるため本論文の成果はいずれも同時実行安全性および耐漏洩安全性を満たす秘密計算の実現コスト解明に貢献するものと見ることができ，そのため本論文の一連の成果は秘密計算の一般性を通じて同時実行安全性および耐漏洩安全性の実現コスト解明という基本的問題に対する一般的結果につながるものである。

具体的には，本論文では以下の四つの結果が示されている。

・第一の結果は同時実行安全ゼロ知識証明に関するものであり，最も強力な同時実行安全性を満たすゼロ知識証明（statistical concurrent non-malleableゼロ知識証明）を通常のゼロ知識証明と全く同じ仮定から構成できることを示すことにより，ゼロ知識証明における最も強力な同時実行安全性が仮定について追加のコスト無しで実現できるという最も理想的な結論を示している。

・第二の結果は耐漏洩ゼロ知識証明に関するものであり，定数ラウンド耐漏洩ゼロ知識証明を非常に弱い標準的仮定（衝突困難ハッシュ関数の存在）から構成できることを示すことで，耐漏洩ゼロ知識証明においてラウンド効率と仮定の両方を同時に低コスト化することが可能という望ましい結果を得ている。

・第三の結果は同時実行安全ゼロ知識証明に関するものであり，特に同時実行安全性を満たす非ブラックボックスゼロ知識証明の新たな方式を提案している。本結果はラウンド効率や安全性証明の仮定について既存結果から改善を達成してはいないが，既存結果と比べ簡潔な安全性証明を持つという特徴があるため非ブラックボックスゼロ知識証明を必要とする同時実行安全性の未解決問題の解決に有用となる可能性を持つ。

・第四の結果は同時実行安全秘密計算に関するものであり，効率の面で望ましい特徴であるブラックボックス構成という特徴をもつ同時実行安全秘密計算を従来のものと比べ大きく良いラウンド効率で実現することにより，同時実行安全秘密計算の実現に必要なコストを効率面で大きく改善している。

以上，本論文はゼロ知識証明と秘密計算における高度な安全性の実現について研究した結果をまとめたものであり，当該研究分野の今後の発展に寄与するところが少なくない。よって，本論文は博士（情報学）の学位論文として価値あるものと認める。また，平成３０年２月２２日に実施した論文内容とそれに関連した口頭試問の結果，合格と認めた。

注)論文審査の結果の要旨の結句には、学位論文の審査についての認定を明記すること。

更に、試問の結果の要旨（例えば「平成　年　月　日論文内容とそれに関連した口頭試問を行った結果合格と認めた。」）を付け加えること。

Webでの即日公開を希望しない場合は、以下に公開可能とする日付を記入すること。
要旨公開可能日：　　年　　月　　日以降